Section IV: **Network Security**
Title: **Digital Signatures Security Standard**
Current Effective Date: **June 30, 2008**
Revision History: **May 7, 2008**
Original Effective Date: **June 30, 2008**

Purpose: To protect the integrity of the North Carolina (NC) Department of Health and Human Services (DHHS) data through the use of digital signatures.

STANDARD

1.0 Background

It is the responsibility of the Divisions and Offices to understand what their individual roles and responsibilities are when sending and receiving information digitally or remotely in order to maintain the integrity and authenticity of DHHS data, while providing non-repudiation to validate an individual's identity.

The Divisions and Offices are responsible for all data integrity of any computer system that stores confidential data and/or information. The Division Information Security Official (ISO) must ensure that digital signatures have been applied, where required, and enforced at the Division and Office level. The digital signatures must provide strong and flexible authentication services for individual users and applications, and must be consistent with the architecture standards in the NC Statewide Technical Architecture (STA).

2.0 Managing Keys

The security of a digital signature system is dependent on maintaining the secrecy of the end-user's private keys and the availability of the public keys. It is the responsibility of the Divisions and Offices, with the assistance of the DHHS Privacy and Security Office (PSO), to instruct the end-users how to guard their private keys against unauthorized acquisition. If a situation occurs in which a private key is made public, the end-user will need to follow the Divisions and Offices procedures and guidelines.

The management authority for the digital signatures will be the authority managing the information technology (IT) infrastructure for the Divisions and Offices. Prior to deployment of a public key infrastructure (PKI) in support of issuing digital signatures, a risk assessment and cost analysis must be performed in deciding what suite of software should be used. The PKI solution must interoperate with other PKI solutions at the statewide level and conform to the state policies, procedures, standards, or any applicable federal regulations.

The primary responsibility of providing the data integrity rests with the authority of each Division and Office in conjunction with the NC State Office of Information Technology Services (ITS). The DHHS PSO is available to assist, if necessary.

Reference:

- NC Statewide Information Security Manual, Version No. 1
  - Chapter 2 – Controlling Access to Information and Systems, Section 01: Controlling Access to Information and Systems
    - Standard 020106 – Managing Passwords
  - Chapter 3 – Processing Information and Documents, Section 03: E-mail and the Worldwide Web
    - Standard 030302 – Using and Receiving Digital Signatures

- NC Statewide Technology Architecture
  - Security Domain 2.1.4. – Perform a Risk Management and cost…
  - Security Domain 2.1.7. – Public Key Infrastructure (PKI) Initiatives…
  - Security Domain 2.1.9. – PKI Initiatives Must Store…

- NC DHHS Security Standards
  - Administrative Security Standards
    - Personnel Security Standard

- NC DHHS Policy and Procedure Manual, Section VIII – Security and Privacy, Security Manual
  - IT Operations Security Policy
  - Personnel Security Policy